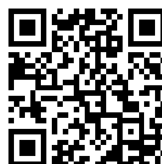






3.

Beiträge
zum
Fermatschen Lehrsatz.

Inaugural-Dissertation

zur

Erlangung der Doctorwürde

von der

Philosophischen Facultät

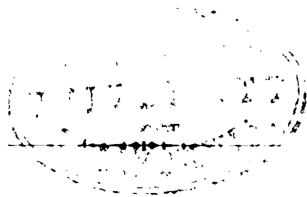
der

Universität zu Giessen

genehmigt.

Verfasser:

Julius Rothholz.



Berlin, 1892.

Buchdruckerei der „Volks-Zeitung“, Actien-Gesellschaft.

Lützowstrasse 105.

Meinen Eltern

in dankbarer Verehrung

gewidmet

vom Verfasser.

Unter den vielen wichtigen von Fermat entdeckten und ohne Beweis der mathematischen Welt hinterlassenen arithmetischen Sätzen hat keiner so lange den Bemühungen der grössten Mathematiker widerstanden, als jener berühmte Satz, wonach die Summe zweier n-ten Potenzen ganzer Zahlen niemals selbst eine solche Potenz sein kann, wenn $n > 2$ ist. Fermat, Euler, Legendre, Lejeune Dirichlet und Lamé haben nur Spezialfälle dieses Problems für n = 4, 3, 5, 14 und 7 bewiesen, und selbst der Weg, auf dem Herr Prof. Kummer so glänzende Resultate für den Fermatschen Satz gewann, hat bis zur Gegenwart noch zu keinem vollständigen Beweise desselben geführt. Die allgemeinen Beweise aber für das in Rede stehende Problem, die in den letzten Jahrzehnten veröffentlicht wurden, können auf Genauigkeit und Richtigkeit keinen Anspruch erheben. Einem Uebelstande, der etwa darin zu suchen wäre, dass der Fermatsche Satz eigentlich eine negative Behauptung enthält, sucht eine an der Berliner Universität gestellte Preisaufgabe abzuhelfen.

In dieser wird die Frage aufgeworfen, von welchem Grade mindestens eine ganze, ganzzahlige rationale Funktion von x sein muss, damit die aus ihr und $x^n - 1$ gebildete Resultante die n-te Potenz einer ganzen Zahl sein kann. Wenn wir nämlich $a^n + b^n$ als die Resultante aus $x^n - 1$ und $a + bx$ auffassen, und, wenn ferner gezeigt werden könnte, dass, falls die Resultante aus $x^n - 1$ und einer ganzen ganzzahligen rationalen Funktion eine n-te Potenz einer ganzen Zahl werden soll, die ganze, ganzzahlige rationale Funktion vom höherem als dem 1. Grade sein müsste, dann wäre der Fermatsche Satz bewiesen. Denn da nur dann die Resultante aus $x^n - 1$ und einer ganzen, ganzzahligen rationalen Funktion von höherem als dem 1. Grade eine n-te Potenz einer ganzen Zahl sein kann, wird die Summe $a^n + b^n$, die ja gerade die Re-

sultante aus $x^n - 1$ und der ganzen, ganzzahligen Funktion ersten Grades $a + bx$ ist, eine n-te Potenz einer ganzen Zahl nicht sein können, womit der Fermatsche Satz bewiesen wäre. Leider hat die wiederholt gestellte Preisaufgabe eine Bearbeitung nicht gefunden, selbst nicht einmal für den Spezialfall $n = 5$, und es ist auch fraglich, ob in dieser positiv gehaltenen Fassung der allgemeine Beweis des Fermatschen Satzes erleichtert wird. Einen allgemeinen Beweis des Fermatschen Satzes enthält auch meine Arbeit nicht, ich will vielmehr bestimmte Zahlenklassen namhaft machen, für die die Allgemeingültigkeit desselben sich zeigen lässt. Nebenher soll auch die Richtigkeit des Fermatschen Satzes für gewisse Exponenten n gezeigt werden. Diesen Auseinandersetzungen wird sich eine Angabe der bisher erledigten Fälle des Fermatschen Problems und eine Kritik einiger verfehlten, allgemeinen Beweise desselben anschliessen.

I.

Professor Kummer beweist im 17. Bande des Crelleschen Journals folgendes Theorem:

Wenn n eine Primzahl ist, und x und y relativ prim untereinander sind, so können die Grössen $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ keinen gemeinschaftlichen Faktor, ausser dem Faktor n haben. Wenn aber $x^n \pm y^n$ den Faktor n enthält, so muss er auch in $x \pm y$ enthalten sein, und zwar übertrifft die Anzahl der Faktoren n in $x^n \pm y^n$ die der Faktoren n in $x \pm y$ um die Einheit. Professor Kummer geht von der identischen Gleichung aus:

$$1)\quad \frac{x^n \pm y^n}{x \pm y} = (x \pm y)^{n-1} \mp n(x \pm y)^{n-3} xy$$
$$+ \frac{n(n-3)}{1 \cdot 2} (x \pm y)^{n-5} x^2 y^2$$
$$(\mp 1)^h \frac{n(n-h-1)\ldots(n-2h+1)}{1 \cdot 2 \cdot 3 \ldots h} (x \pm y)^{n-2h-1} x^h y^h$$
$$+ (\mp 1)^{\frac{n-1}{2}} n (xy)^{\frac{n-1}{2}}.$$

Wenn nun $\frac{x^n \pm y^n}{x \pm y}$ und $x \pm y$ einen gemeinschaftlichen Faktor haben, so muss derselbe, wie aus Gleichung (1) ersichtlich ist, auch in dem Gliede $n(xy)$ auf der rechten Seite unserer Gleichung (1) enthalten sein. Weil aber xy und $x \pm y$ relativ prim untereinander sind, kann der grösste gemeinschaftliche Faktor, den die Grössen $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ haben können, nur n sein. Betrachten wir ferner die Coefficienten der rechten Seite unserer Gleichung (1):

$\frac{n}{1}, \frac{n(n-3)}{1 \cdot 2} \ldots \frac{n(n-h-1)\ldots(n-2h+1)}{h!}$, so werden dieselben, da sie ganze Zahlen sind, und die Primzahl n in den Zählern nicht durch die kleineren Faktoren des Nenners gehoben werden kann, durch n theilbar sein. Daraus folgt, dass $x^n \pm y^n$ nur dann den Faktor n enthalten kann, wenn zugleich:

$$x \pm y \equiv o \pmod{n} \text{ ist.}$$

Setzt man ferner $x^n \pm y^n = C\, n^k$ und $x + y = C\, n^\lambda$, so folgt aus der Gleichung (1), dass

$$\lambda = k - 1 \text{ ist.}$$

Eine Anwendung dieses Theorems wollen wir auf die Gleichung:

1) $x^n \pm y^n = z^n$ machen, in der x, y, z relativ prim unter einander sein sollen und n eine ungerade Primzahl bedeutet. Unsere Gleichung (1) lässt sich auch in folgender Form schreiben:

$$2)\ (x \pm y)\left(\frac{x^n \pm y^n}{x \pm y}\right) = z^n.$$

Ist nun

a) $z \not\equiv o$ (mod. n),*) so werden die beiden Faktoren $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ relativ prim untereinander sein; deshalb wird jeder dieser Faktoren eine n-te Potenz sein.

$$3a)\ \left\{\begin{array}{l} x \pm y = z_1^n \\ \frac{x^n \pm y^n}{x \pm y} = z_2^n \end{array}\right\} \text{ für } z_1 z_2 = z.$$

b) Ist aber

$z \equiv o$ (mod. n^h), so müssen nach (1) die beiden Faktoren $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ den Faktor n und zwar können sie ihn nur in der ersten Potenz gemeinsam haben, da die Anzahl der Faktoren n in $x^n \pm y^n$ die der Faktoren n in $x \pm y$ um die Einheit übertrifft. Unsere Gleichung (1) wird dann in folgende Zwei zerfallen

$$3_b)\ \left\{\begin{array}{l} x \pm y = n^{nh-1} z_1^n \\ \frac{x^n \pm y^n}{x \pm y} = n z_2^n, \text{ wenn} \end{array}\right.$$

$n^h z_1 z_2 = z$ ist.

II.

Im Anschlusse an die Ergebnisse des vorigen Abschnitts wollen wir die Gleichung

$x^n \pm y^n = z^n$ untersuchen, wenn z eine Primzahl oder Primzahlpotenz und n eine ungrade Primzahl ist.

Angenommen, es bestände die Gleichung

1) $x^n \pm y^n = z^n$ oder

2) $(x \pm y)\left(\frac{x^n \pm y^n}{x \pm y}\right) = z^n$, dann haben wir zwei Fälle zu unterscheiden

a) $z \not\equiv o$ mod. n. Weil nun x und y relativ prim untereinander sind, werden in diesem Falle die beiden Faktoren $(x \pm y)$ und $\left(\frac{x^n \pm y^n}{x \pm y}\right)$ n te Potenzen sein müssen, und weil z ferner nur einen Primzahlfaktor enthält, werden wir erhalten:

*) Das Zeichen $\not\equiv$ bedeute in dieser Arbeit incongruent.

$$3)\quad \begin{matrix} x \pm y \\ \dfrac{x^n \pm y^n}{x \pm y} \end{matrix} = \left\{ \begin{matrix} 1 \\ z^n \end{matrix} \right.$$

b) Ist aber $z = n^h$, so werden die beiden Faktoren $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ den Faktor n gemeinschaftlich haben können; und wir erhalten, unter Berücksichtigung der Resultate auf Seite 4 Gl. 3_b folgende Gleichungen:

$$4)\quad x \pm y = n^{nh-1} = \frac{z^n}{n}$$

$$\frac{x^n \pm y^n}{x \pm y} = n.$$

α) Es ist unmöglich die Gleichung

1) $x^n + y^n = z^n$ durch ganze positive Zahlen, die relativ prim untereinander sind, zu befriedigen. Denn für $z \not\equiv 0$ (mod. n) kann nach der Gleichung (3) $x + y$ die Werte $x + y = \left\{ \begin{matrix} 1 \\ z^n \end{matrix} \right.$ annehmen. Ist aber $x + y = 1$, so könnte $\begin{matrix} x \\ y \end{matrix} = \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right.$ nur werden, Werte für x und y, die unsere Gleichung (1) nicht befriedigen. Wenn ferner $x + y = z^n$ wäre, so würde $\frac{x^n + y^n}{x + y} = 1 < x + y$ sein, was wiederum unmöglich ist. Wenn aber $z = n^h$ ist, so ist nach Gleichung (4) $x + y = \frac{z^n}{n}$ und $\frac{x^n + y^n}{x + y} = n$, folglich $x + y > \frac{x^n + y^n}{x + y}$, was unmöglich ist.

β) Ist in der Gleichung

1′) $x^n - y^n = z^n$, wo x, y, z ganze positive Zahlen bedeuten, $z = n^h$, so wäre nach Gleichung (4)

$$x - y = \frac{z^n}{n},\ \frac{x^n - y^n}{x - y} = n, \text{ folglich wäre}$$

$$x - y > \frac{x^n - y^n}{x - y}, \text{ was unmöglich ist.}$$

Ist aber $z \not\equiv 0$, so könnte nach der Gleichung (3) erstens $x - y = z^n$ sein, dann wäre aber $\frac{x^n - y^n}{x - y} = 1 < x - y$, was unmöglich ist. Zweitens könnte aber $x - y$ den Wert

$$x - y = 1 \text{ annehmen.}$$

Alsdann müsste

2′) $x = z + t$, $y = z + t - 1$ werden, wo t und $t - 1$ ganze Zahlen bedeuten, die ebenso wie x und y relativ prim zu z sein müssen. Setzen wir für x und y ihre Werte aus (2′) in die Gleichung (1′) ein, so erhalten wir die Gleichung:

$$3')\quad (z + t)^n - (z + (t - 1))^n = z^n.$$

Aus dieser Gleichung erschliessen wir die Congruenz

4') $t^n \equiv (t-1)^n$ (mod. z) oder auch

5') $t^n \equiv (t-1)^n$ (mod. p), wenn p der in z enthaltene Primzahlfaktor ist. Falls nun

$p \not\equiv 1$ (mod. n), also $p-1$ und n keinen gemeinschaftlichen Teiler haben, kann man eine positive ungrade Zahl α so bestimmen, dass

6') $\alpha n \equiv 1 \bmod \varphi(p)$ wird, wo $\varphi(p) = p-1$ das Gausssche Zeichen bedeutet. Aus der Congruenz (5') ergiebt sich auch folgende.

7') $t^{\alpha n} \equiv (t-1)^{\alpha n}$ (mod. p). Da aber nach (6') $\alpha n = \lambda\varphi(p) + 1$ ist, und da ferner nach (2') t und $t-1$ zu z bezw. zu p relativ prim sind, wird nach dem bekannten Fermatschen Satze:

$t^{\alpha n} \equiv t$, $(t-1)^{\alpha n} \equiv t-1$ (mod. p) sein. Aus der Congruenz (7') ergiebt sich dann:

8') $t \equiv t-1$ (mod p) oder

$1 \equiv o$ (mod. p), eine Congruenz, die nicht möglich ist. Falls jedoch $p \equiv 1$ (mod. n), $p-1$ also durch n teilbar ist, können wir einen solchen Schluss nicht ziehen; dann wollen wir aber zeigen, dass die Gleichung

1'') $x^{2n} - y^{2n} = z^{2n}$ nicht durch ganze Zahlen befriedigt werden kann, selbst wenn der Primzahlfaktor p von z, $p \equiv 1$ mod. n ist. Die linke Seite unserer Gleichung 1'') können wir in ein Differenzenprodukt umformen:

2'') $(x^n - y^n)(x^n + y^n) = z^{2n}$. Die beiden Faktoren der linken Seite dieser Gleichung sind relativ prim untereinander, und da z nur einen Primzahlfaktor enthalten soll, und $x^n + y^n > x^n - y^n$ ist, wird $x^n - y^n = 1$ sein müssen, was unmöglich ist für $n > 2$.

Damit haben wir gezeigt, dass eine 2n-te Potenz einer Primzahl oder Primzahlpotenz sich nicht in die Differenz zweier 2n-ten Potenzen von ganzen Zahlen zerlegen lässt; in die Summe zweier 2n-ten Potenzen ist sie auch nicht zerlegbar, da $x^n + y^n = z^n$ sich nicht durch ganze Zahlen befriedigen lässt, wenn z eine Primzahl oder Primzahlpotenz ist, folglich können wir jetzt sagen: Die Gleichung

$x^{2n} \pm y^{2n} = z^{2n}$ kann nicht durch ganze Zahlen befriedigt werden, wenn eine der Zahlen x, y, z eine Primzahl ist und n eine ungrade Primzahl bedeutet.

Die Gleichung

$x^n + y^n = z^n$ wird, wenn n eine ungrade Primzahl ist, nach unsern Auseinandersetzungen in diesem Abschnitte durch ganze Zahlen nicht befriedigt werden können, wenn x, y oder z eine Potenz einer solchen Primzahl ist, die $\not\equiv 1$ (mod n) ist.

III.

Das Ergebniss des vorigen Abschnittes wollen wir zu dem Beweise verwenden, dass sich die 2n-te Potenz eines Produktes aus zwei ungraden Primzahlen oder Primzahlpotenzen nicht in die Differenz zweier 2n-ten Potenzen zerlegen lässt, wenn n eine ungrade Primzahl bedeutet.

1) $x^{2n} - y^{2n} = z^{2n} = (p_1^{\alpha_1} p_2^{\alpha_2})^{2n}$

Die Unmöglichkeit der Gleichung (1), wenn n, p_1 und p_2 ungrade Primzahlen sind, ergiebt sich aus Folgendem: Unsere Gleichung (1) lässt sich auch in folgender Form schreiben:

2) $(x^n - y^n)(x^n + y^n) = (p_1^{\alpha_1} p_2^{\alpha_2})^{2n}$. Da x und y relativ prim sind, z aber ungrade ist, müssen die beiden Faktoren $x^n - y^n$ und $x^n + y^n$ zu einander relativ prim sein. Weil aber ferner für $n > 2$

$x^n - y^n > 1$ sein muss, und jeder der Faktoren eine 2n-te Potenz werden muss, wird

$x^n - y^n = (p_1^{2\alpha_1})^n$, $x^n + y^n = (p_2^{2\alpha_2})^n$ werden, wenn $p_2^{\alpha_2} > p_1^{\alpha_1}$ ist. Wir haben aber gezeigt, dass die n-te Potenz einer Primzahlpotenz nicht in die Summe zweier n-ten Potenzen ganzer Zahlen zerlegbar ist, folglich kann die Gleichung

$x^n + y^n = (p_2^{2\alpha_2})^n$ nicht durch ganze Zahlen befriedigt werden, und damit auch nicht unsere Gleichung (1).

IV.

Wir wollen in diesem Abschnitte nachweisen, dass die Gleichung

$x^n + y^n = (2p)^n$ durch ganze Zahlen nicht befriedigt werden kann, wenn n und p ungrade Primzahlen sind. Aus unserer Gleichung

1) $x^n + y^n = (2p)^n$ ergeben sich auch die beiden andern:

2) $x^n = (2p)^n - y^n$

3) $y^n = (2p)^n - x^n$

a) Ist nun $p \not\equiv 0 \pmod{n}$, so folgt aus der Gleichung (1)

$x + y = 2^n$

4) $\frac{x^n + y^n}{x + y} = p^n$. Aus der Gleichung 2) schliessen wir, je nachdem $x \equiv 0$, oder $x \not\equiv 0 \pmod{n}$ ist

für $x \not\equiv 0 \pmod{n}$:

$$\left.\begin{aligned} 2p - y &= x_1^n \\ 5)\ \frac{(2p)^n - y^n}{2p - y} &= x_2^n \end{aligned}\right\} \text{für } x_1 x_2 = x$$

für $x \equiv 0 \pmod{n^h}$:

$$\left.\begin{aligned} 2p - y &= n^{nh-1} x_1^n \\ 5')\ \frac{(2p)^n - y^n}{2p - y} &= x_2^n \end{aligned}\right\} \text{für } n^h x_1 x_2 = x$$

Ebenso schliessen wir aus der Gleichung (3), je nachdem $y \equiv o$ oder $y \not\equiv o$ (mod. n) ist,

für $y \not\equiv o$ (mod. n)

$$6) \left.\begin{array}{l} 2p - x = y_1^n \\ \dfrac{(2p)^n - x^n}{2p - x} = y_2^n \end{array}\right\} \text{für } y_1 y_2 = y$$

für $y \equiv o$ (mod. n^{h_1})

$$6') \left.\begin{array}{l} 2p - x = n^{nh_1 - 1} y_1^n \\ \dfrac{(2p)^n - x^n}{2p - x} = n y_2^n \end{array}\right\} \text{für } n^{h_1} y_1 y_2 = y$$

Ist $x, y, p \not\equiv o$ (mod. n), so gelten für unsere Zerlegungen die Gleichungen 4, 5. und 6. Addieren wir die ersten dieser drei Gleichungssysteme, so erhalten wir

$$7) \left\{\begin{array}{l} x + y = 2^n \\ 2p - y = x_1^n \\ 2p - x = y_1^n \\ \hline 4p = 2^n + x_1^n + y_1^n \end{array}\right.$$

x_1^n und y_1^n können gleichzeitig nicht $= 1$ werden, weil sonst aus den Gleichungen $\left.\begin{array}{l} 2p - y = x_1^n = 1 \\ 2p - x = y_1^n = 1 \end{array}\right\} x = y$ sich ergeben würde, Werte für x und y, die unsere Gleichung (1) unmöglich machen. Da x_1 und y_1 ganze Zahlen sein sollen, so folgt daraus, dass entweder x_1 oder $y_1 \geqq 2$ sein muss.

Aus der Gleichung (7) erhalten wir dann folgende Ungleichung

$$8) \; 4p > 2^n + 2^n = 2^{n+1} \text{ oder}$$
$$p > 2^{n-1}$$

Ist x oder $y \equiv o$ (mod. n), beide Grössen können es nicht gleichzeitig sein, weil x und y relativ prim sein sollen, so muss das Gleichungssystem (5) durch das (5′), oder das Gleichungssystem (6) durch das von (6′) ersetzt werden. Wäre z. B. $x \equiv o$ (mod. n^h), dann addiren wir folgende drei Gleichungen aus den Gleichungssystemen 4) 5′) 6)

$$\begin{array}{l} x + y = 2^n \\ 2p - y = n^{nh-1} x_1^n \\ 2p - x = y_1^n \\ \hline \end{array}$$

9) $4p = 4p = 2^n + n^{nh-1} x_1^n + y_1^n$; in diesem Falle könnte $x_1 = y_1 = 1$ zwar werden, allein, da $n \geqq 3$ ist, wird immer $n^{nh-1} > 2^n$ sein, selbst wenn h den kleinsten Werth, $h = 1$, annimmt. Wir erhalten also aus der Gleichung 9) eine der Ungleichung 8) entsprechende

$$8') \; 4p > 2^{n+1}, \; p > 2^{n-1}$$

Ganz dieselbe Ungleichung würde sich ergeben, wenn $y \equiv o$ (mod. n^{h_1}) wären und wir die ersten Gleichungen aus den Systemen 4, 5 und 6′) addiren müssten. Aus der Gleichung 1) ergiebt sich, dass die Summe aus x und y : 9)

$$x + y > 2p \text{ werden muss.}$$

Nach der Gleichung (4) ist $x + y = 2^n$; aus der Ungleichung (9) ergiebt sich dann folgende:

$$10)\ 2^n > 2p$$
$$11)\ p < 2^{n-1}.$$

Die Ungleichungen für p aus (8) und (8') $p > 2^{n-1}$ widersprechen der eben gefundenen $p < 2^{n-1}$, folglich ist unsere Gleichung (1) durch ganze Zahlen nicht erfüllbar.

b) Ist $p \equiv o \pmod{n}$, so würde aus unserer Gleichung (1), da x und y ungrade sind, folgen

$$2')\ x + y = 2^n p^{n-1},\quad \frac{x^n + y^n}{x + y} = p;$$

denn $\frac{x^n + y^n}{x + y} = x^{n-1} \ldots + y^{n-1}$ ist in diesem Falle ungrade. Es müsste demnach $x + y > \frac{x^n + y^n}{x + y}$ sein, was unmöglich ist.

V.

Die Gleichung

$x^{2n} + y^{2n} = z^{2n}$ soll untersucht werden, wenn n eine ungerade Primzahl bedeutet und x, y, z wie bisher relativ prim untereinander sind.

1) Wir zeigen zuerst, dass die 2n-te Potenz einer graden Zahl sich nicht in die Summe zweier 2n-ten Potenzen von ganzen, positiven Zahlen zerlegen lässt. Gesetzt, es wäre $z = 2z_1$ und x und y relativ prim zu z, so wollen wir zeigen, dass die Gleichung

1) $x^{2n} + y^{2n} = z^{2n} = (2z_1)^{2n}$ nicht durch ganze positive Zahlen befriedigt werden kann. Weil z grade ist und x und y relativ prim zu z sind, müssen x und y ungrade Zahlen sein. Das Quadrat einer ungraden Zahl hat aber die Form $4l + 1$; deshalb werden auch $x^{2n} = (x^n)^2$ und $y^{2n} = (y^n)^2$ von dieser Form sein; und ihre Summe $x^{2n} + y^{2n}$ wird demnach die Form $4l' + 2$ haben, wo l und l' ganze Zahlen bedeuten. Nach unserer Gleichung (1) $x^{2n} + y^{2n} = (2z_1)^{2n}$ ist aber die Summe $x^{2n} + y^{2n}$ gleich dem Quadrate einer graden Zahl $(2z_1)^n$; sie hat also die Form $4l''$, daraus ergiebt sich, dass unsere Gleichung (1) durch ganze Zahlen, die relativ prim untereinander sind, nicht befriedigt werden kann.

2) Die Primzahl n in unserm Exponenten 2n habe nunmehr die Form $4k + 3$. Dann können wir zeigen, dass die 2n-te Potenz einer graden Zahl auch nicht in die Differenz zweier 2n-ten Potenzen von ganzen positiven Zahlen, die relativ prim untereinander sind, zerlegbar ist. Unsere zu untersuchende Gleichung wird also folgende sein:

2) $x^{2n} - y^{2n} = (2z_1)^{2n} = z^{2n}$, wo n eine Primzahl von der Form $4k + 3$ sein soll. Die Zahlengrössen x und y werden un-

grade sein, da sie zu $z = 2z_1$ relativ prim sein sollen. Wir haben zwei Fälle zu unterscheiden, je nachdem $z \equiv o \pmod{n}$ oder $z \not\equiv o \pmod{n}$ ist.

a) Ist $z \not\equiv o \pmod{n}$, dann sind die beiden Faktoren der linken Seite unserer Gleichung (2) $x^2 - y^2$ und $\frac{x^{2n} - y^{2n}}{x^2 - y^2}$ relativ prim untereinander, folglich wird jeder von ihnen eine 2n-te Potenz sein müssen. Wir erhalten demnach folgende Gleichungen:

$$3) \quad \left\{ \begin{array}{l} x^2 - y^2 = 2^{2n} z_2^{2n} \\ \frac{x^{2n} - y^{2n}}{x^2 - y^2} = z_3^{2n} \end{array} \right\} \text{ für } z_2 z_3 = z_1.$$

z_3 kann den Faktor 2 nicht enthalten, weil $\frac{x^{2n} - y^{2n}}{x^2 - y^2}$ relativ prim zu $x^2 - y^2$ ist, $x^2 - y^2$ als Differenz zweier ungrader Quadrate aber grade ist.

Es ist aber

$$4) \quad \frac{x^{2n} - y^{2n}}{x^2 - y^2} = \sum_{\nu=0}^{n-1} x^{2(n-1-\nu)} y^{2\nu} = \sum_{\nu=0}^{n-1} (x^{n-1-\nu} y^{\nu})^2.$$

Unsere Summe (4) setzt sich also aus n Quadraten von Ausdrücken der Form $x^{n-1-\nu} y^{\nu}$, wo ν die Werte o, 1, ... n — 1 annehmen kann, zusammen, die, weil x und y ungrade Grössen sind, selber ungrade sind. Da aber das Quadrat einer ungraden Zahl die Form $4l + 1$ hat und n unserer Annahme nach $n = 4k + 3$ ist, wird die Summe (4) $\sum_{\nu=0}^{n-1} (x^{n-1-\nu} y^{\nu})^2$ aus den $(4k + 3)$ Gliedern von der Form $4l + 1$ selbst die Form $4l' + 3$ haben. Nach der Gleichung (3) ist aber $\sum_{\nu=0}^{n-1} (x^{n-1-\nu} y^{\nu})^2 = \frac{x^{2n} - y^{2n}}{x^2 - y^2}$ das Quadrat der ungraden Zahl z_3^n, also von der Form $4l'' + 1$, folglich lässt sich unsere Gleichung (2) nicht durch ganze Zahlen, die relativ prim untereinander sind, befriedigen.

b) Ist $z \equiv o \pmod{n^h}$, so wird nach dem Abs. I

$$3') \quad \left\{ \begin{array}{l} x^2 - y^2 = 2^{2n} n^{2nh-1} z_2^n \\ \frac{x^{2n} - y^{2n}}{x^2 - y^2} = n z_3^n \end{array} \right\} \text{ für } n^h z_2 z_3 = z_1.$$

Da x und y den Faktor n nicht enthalten können, weil sie zu z relativ prim sind, erhalten wir nach dem gewöhnlichen Fermatschen Satz

5) $x^{n-1} \equiv y^{n-1} \equiv 1 \pmod{n}$ oder

6) $x^{2(n-1)} \equiv y^{2(n-1)} \equiv 1 \pmod{n}$.

Daraus folgt, dass

$$7)\quad \left.\begin{aligned} x^{2n} &\equiv x^{2(n-1)+2} \equiv x^2 \\ y^{2n} &\equiv y^{2(n-1)+2} \equiv y^2 \end{aligned}\right\} \text{(mod. n) wird.}$$

Wir erhalten demnach

$$8)\quad \frac{x^{2n} - y^{2n}}{x^2 - y^2} \equiv \frac{x^2 - y^2}{x^2 - y^2} \equiv 1 \pmod{n}.$$

Nach 3′) ist

$\dfrac{x^{2n} - y^{2n}}{x^2 - y^2} \equiv o$ (mod. n), folglich würde sich aus (8) die Congruenz

$$o \equiv 1 \text{ (mod. n) ergeben, die unmöglich ist.}$$

Damit haben wir gezeigt, dass, wenn n eine Primzahl von der Form $4k + 3$ ist, die 2n-te Potenz einer graden Zahl nicht in die Differenz von zwei 2n-ten Potenzen ganzer Zahlen zerlegbar ist; weil nun eine 2n-te Potenz einer graden Zahl sich, wie wir gezeigt hahen, auch nicht in die Summe zweier 2n-ten Potenzen von ganzen Zahlen zerlegen lässt, können wir jetzt folgenden Satz aussprechen:

Ist n eine Primzahl von der Form $4k + 3$, so lässt sich die 2n-te Potenz irgend einer Zahl weder in die Summe noch in die Differenz von zwei 2n-ten Potenzen ganzer Zahlen zerlegen, denn eine der Zahlen x, y, z muss grade sein; es kann demnach die Gleichung

$x^{2n} + y^{2n} = z^{2n}$ nicht durch ganze Zahlen befriedigt werden.

Das Resultat, das Dirichlet durch seinen Beweis für den Spezialfall $n = 14$ gewonnen hat, ist in dem obigen von uns gefolgerten enthalten, da $14 = 2 . 7 = 2\,(4 . 1 + 3)$ ist.

Haben wir jetzt ganz allgemein die Gleichung

$x^{2n} + y^{2n} = z^{2n}$, wo n und z jede ungrade Primzahl bedeuten kann, so wird dieselbe durch ganze Zahlen x, y, z, die relativ prim untereinander sein sollen, nicht erfüllt werden können, wenn z einen Primzahlfaktor von der Form $4k + 3$ enthält, weil sich kein Quadrat einer Zahl, die einen Primzahlfaktor von der Form $4k + 3$ enthält, in die Summe zweier Quadrate von Zahlen, die relativ prim zu ihr sind, zerlegen lässt.

VI.

Wir wollen in diesem Abschnitt die Gleichung

$x^n + y^n = z^n$ untersuchen, wenn n eine ungrade Primzahl bedeutet und x, y, z relativ prim untereinander sind.

Aus der Gleichung

1) $x^n + y^n = z^n$ folgt nach dem ersten Abschnitt,

a) wenn $z \not\equiv o \pmod{n}$ ist,

$$\left.\begin{array}{l} x \pm y = z_1^n \\ \dfrac{x^n \pm y^n}{x \pm y} = z_2^n \end{array}\right\} \text{für } z_1 z_2 = z$$

b) wenn $z \equiv o \pmod{n^h}$ ist,

$$\left.\begin{array}{l} x \pm y = n^{nh-1} z_1^n \\ \dfrac{x^n \pm y^n}{x \pm y} = n z_2^n \end{array}\right\} \text{für } n^h z_1 z_2 = z$$

Die Faktoren der linken Seite unserer Gleichung (1) $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ sind, wenn $z \not\equiv o \pmod{n}$ ist, zu einander relativ prim. Daraus ergiebt sich, dass kein Faktor von z_2 in z_1 resp. in $x \pm y$ enthalten sein kann. Aber selbst, wenn $z \equiv o \pmod{n^h}$ ist, und $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y}$ den gemeinschaftlichen Faktor n haben können, wird nach der von uns gewählten Bezeichnungsweise in den Gleichungen (1_b) z_1 resp. $x \pm y$ durch keinen Faktor von z_2 theilbar sein können. Liesse sich zeigen, dass wir aus der Gleichung (1) eine Congruenz erschliessen können, die besagt, dass $x \pm y$ resp. z_1 durch einen oder mehrere Faktoren von z_2 theilbar ist, so würden wir auf einen Widerspruch stossen mit dem Vorhergehenden und damit die Unmöglichkeit unserer Gleichung (1) erwiesen haben. Da der Faktor $\frac{x^n \pm y^n}{x \pm y} > (x \pm y)$ sein muss, können wir in beiden Fällen, sowohl, wenn $z \not\equiv o \pmod{n}$, als auch, wenn $z \equiv o \pmod{n^h}$ ist, aus den Gleichungen unter (1a) und (1_b) erschliessen, dass z_2 Faktoren enthalten muss, die grösser als 1 sind; diese Faktoren von z_2 werden sämmtlich ungrade Zahlen sein, weil $\frac{x^n \pm y^n}{x \pm y}$ selbst ungrade ist, ganz gleich, welche von den Zahlengrössen x, y, z auch immer grade ist. Nennen wir nun irgend einen der in z_2 enthaltenen Primzahlfaktoren f, wo $f > 2$ ist, so kann z_1 nicht durch f theilbar sein. Wir erhalten

2) $z_1 \not\equiv o \pmod{f}$.

Aus unserer Gleichung (1) folgt die Congruenz

3) $x^n \equiv \mp y^n \pmod{z}$. Aus dieser Congruenz ergeben sich die folgenden:

3') $x^n \equiv \mp y^n \pmod{z_2}$

3'') $x^n \equiv \mp y^n \pmod{f}$, da z_2 und f Faktoren von z sind.

Liesse sich nun durch eine diophantische Gleichung eine ungrade Zahl α so bestimmen, dass

4) $\alpha n \equiv 1 \pmod{\varphi[f]}$ ist, wo $\varphi(f) = f - 1$ das Gausssche

Zeichen bedeutet, so würde aus der Congruenz 3'') auch folgende Congruenz folgen:

5) $x^{\alpha n} \equiv + y^{\alpha n}$ (mod. f). Da aber x und y relativ prim zu z und folglich auch zu f sind, weiss man nach dem bekannten Fermatschen Satze, dass

$x^{f-1} \equiv y^{f-1} \equiv 1$ (mod. f) ist. Nach der Gleichung (4) soll aber

$\alpha n = \lambda (f-1) + 1$ sein, wo λ eine ganze Zahl bedeutet, folglich ergiebt sich aus (5) die weitere Congruenz

6) $x \equiv \mp y$ (mod. f) oder
7) $x \pm y \equiv o$ (mod. f).

Diese Congruenz widerspricht unserer Congruenz (2), woraus dann die Unmöglichkeit der Gleichung (1) folgt. Es fragt sich deshalb, in welchen Fällen die diophantische Gleichung (4) durch ganze Zahlen lösbar sein wird. Wir werden nunmehr die einzelnen Fälle zu durchsprechen haben.

α) n ist eine ungrade Primzahl. Sobald n grösser sein wird, als irgend einer der in z_2 vorkommenden Primzahlfaktoren, oder allgemeiner, da wir die Faktoren von z_1 und z_2 nicht näher kennen, sobald n grösser sein wird, als jeder der in z vorkommenden Primzahlfaktoren, wird sich die diophantische Gleichung (4) lösen lassen, weil dann n und φ (f) keinen gemeinschaftlichen Faktor haben können. Wir kommen deshalb zu folgendem Resultat:

Die n-te Potenz irgend einer ganzen Zahl lässt sich nicht in die Summe zweier n-ten Potenzen ganzer Zahlen zerlegen, wenn n grösser als jeder der in ihr enthaltenen Primzahlfaktoren ist.

β) Enthält z nur Primzahlfaktoren von der Form $2^k + 1$ und den Faktor 2^{k_1}, wo k und k_1 ganze Zahlen einschliesslich der Null bedeuten, so wird unsere Congruenz (4) sich ebenfalls lösen lassen. Denn weil

$$\frac{x^n \pm y^n}{x \pm y} = x^{n-1} \mp x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1}$$

immer eine ungrade Zahl ist und z_2 deshalb nur Faktoren von der Form $2^k + 1$ enthält, wird $\varphi(2^k + 1) = 2^k$ mit n keinen gemeinschaftlichen Faktor haben. Wir erhalten also folgendes Resultat:

Die n-te Potenz einer ganzen Zahl, die ausser einem Faktor 2^{k_1} nur noch Primzahlfaktoren von der Form $2^k + 1$ enthält, lässt sich weder in die Summe noch in die Differenz zweier n-ten Potenzen von ganzen Zahlen zerlegen:

γ) Herrn Professor Kummer ist es vermöge seiner Theorie der idealen complexen Zahlen gelungen, zu beweisen, dass die Gleichung

$x^n \pm y^n = z^n$ sich für eine ganze Reihe von wohl charakterisierten Primzahlexponenten, unter denen sich alle Primzahlen des Zahlenintervalls von 1—100 befinden, durch ganze Zahlen nicht erfüllen lässt.

Benutzen wir diesen von Herrn Professor Kummer gegebenen Beweis, so können wir weiter folgende Schlussfolgerungen ziehen:

Enthält z ausser den Primzahlfaktoren aus dem Zahlenintervall von 1—100 solche Primzahlfaktoren, die aus der Summe eines Produktes von Primzahlen oder deren Potenzen aus demselben Zahlenintervall und der Einheit gebildet sind, z. B.

$$2^{k_2} 3^{k_3} 5^{k_5} \ldots + 1,$$

so wird sich unsere Gleichung (1) auch nicht durch ganze Zahlen erfüllen lassen. Denn enthält z_2 nur Primzahlfaktoren von der Form $2^k + 1$, so ist nach (β) die Gleichung (1) unmöglich; enthält aber z_2 die andern charakterisierten Primzahlfaktoren, so wird in allen den Fällen, wo $\varphi(f) \equiv o \pmod{n}$ ist, n kleiner als eine Primzahl des Zahlenintervalls von 1—100 oder auch einer derselben gleich sein, weil $\varphi(f)$ wegen der von uns getroffenen Beschränkung der in z vorkommende Primzahlfaktor nur Primzahlen des Zahlenintervalls von 1—100 enthalten kann; für solche n ist aber die Unmöglichkeit unserer Gleichung (1) durch den Kummerschen Beweis erwiesen. Ist dagegen n grösser als 97, so wird sich die diophantische Gleichung (4) immer lösen lassen. Wir erhalten also folgendes Resultat:

Die n-te Potenz einer Zahl, die ausser den Primzahlfaktoren des Zahlenintervalles von 1—100 nur solche Primzahlfaktoren enthält, die von der Form

$$2^{k_2} 3^{k_3} 5^{k_5} - 97^{k_{97}} + 1 \text{ sind, wo } k_2 > o,\ k_3 \ldots k_{97}$$

ganze Zahlen inclus. der Null bedeuten, lässt sich nicht in die Summe oder Differenz zweier n-ten Potenzen von ganzen Zahlen zerlegen.

δ) Unsere diophantische Gleichung (4) wird sich auch dann immer lösen lassen, wenn z nur solche Primzahlfaktoren enthält, die $\not\equiv 1 \pmod{n}$ sind. Denn da f auch ein Primzahlfaktor von z ist, wird

$f \not\equiv 1 \mod n$ sein, folglich wird

$\varphi(f) = f - 1 \not\equiv 0 \pmod{n}$. Demnach wird sich unsere diophantische Gleichung (4) lösen lassen, und wir erhalten folgendes Resultat:

Die n-te Potenz einer ganzen Zahl, deren Primzahlfaktoren $\not\equiv 1 \pmod{n}$ sind, ist nicht in die Summe zweier n-ten Potenzen ganzer Zahlen zerlegbar.

ε) Enthält schliesslich z_2 nur einen Primzahlfaktor, der $\not\equiv 1$

(mod. n) ist, so wird sich wie in den vorhergehenden Fällen die Unmöglichkeit unserer Gleichung (1) ergeben.

Nur dann, wenn z_2 ausschliesslich Primzahlfaktoren von der Form $\lambda n + 1$ enthält, können wir unsere diophantische Gleichung (4) nicht lösen.

Für solche Zahlen z das Fermatsche Problem in seiner Allgemeinheit streng zu beweisen, haben wir bisher keinen Weg gefunden. Es fragt sich aber, wenn wir aus unserer Gleichung (1)

1) $x^n \pm y^n = z^n$ die beiden andern

1') $x^n = z^n \mp y^n$

1'') $y^n = \pm z^n \mp x^n$ ableiten und dann die üblichen Faktorenzerlegungen vornehmen, ob man nicht beweisen könnte, dass, wenn zwei von den einander entsprechenden Grössen x_2, y_2, z_2 z. B. z_2 und x_2 nur Primzahlfaktoren von der Form $\lambda n + 1$ enthalten, die dritte y_2 nicht notwendiger Weise auch Primzahlfaktoren enthalten muss, die $\not\equiv 1$ mod. n sind.

Mit diesem Nachweise würde der Fermatsche Satz ganz allgemein für alle Zahlen gelten, während uns in diesem Abschnitt nur der Beweis der Giltigkeit des Fermatschen Satzes für bestimmte Zahlenklassen gelungen ist. Unsere Folgerungen im Teile (γ) dieses Abschnittes lassen sich noch dahin erweitern, dass unsere Gleichung

$x^n \pm y^n = z^n$ auch dann unmöglich wird, wenn z ausser den genannten Primzahlfaktoren nur solche von der Form

$2^{k_2} 3^{k_3} 5^{k_5} — \lambda_1^{k_{\lambda_1}} — \lambda_n^{k_{\lambda_n}} + 1$ enthält, wo $\lambda_1 — \lambda_n$ Primzahlen sind, die den Kummerschen Bedingungen für die Giltigkeit des Fermatschen Satzes genügen.

VII.

Die Beweise zu dem Fermatschen Satz.

Um den Beweis des Fermatschen Satzes haben sich eine Reihe deutscher und französischer Mathemathiker, besonders aber in unserem Jahrhundert Herr Professor Kummer verdient gemacht. Der Zeit nach folgen dem Unmöglichkeitsbeweise der Gleichung $x^n + y^n = z^n$ für den Speziälfall $n = 4$ von Fermat selbst der Eulersche Beweis für die Spezialfälle $n = 4$, $n = 3$, der Legendresche Beweis für die Spezialfälle $n = 3$, $n = 5$, der Beweis von Lejeune Dirichlet für den Spezialfall $n = 14$, der Lamésche Beweis für den Spezialfall $n = 7$, von dem der Dirichletsche wiederum ein spezieller Fall ist, und schliesslich der hervorragende Kummersche Beweis, der mit Ausnahme des Falles für $k = 3$ alle vorhergenannten Beweise als Spezialfälle in sich enthält. Der Methode nach unter-

scheiden sich die Spezialbeweise der deutschen Mathematiker Euler und Dirichlet von denen der Franzosen Legendre und Lamé. Euler und Dirichlet zeigen, dass sich unmittelbar oder nach Anwendung eines Kunstgriffes aus der Annahme, dass die Gleichungen

$$x^4 \pm y^4 = z^4$$
$$x^3 \pm y^3 = z^3$$
$$x^{14} \pm y^{14} = z^{14}$$

durch grössere Zahlenwerthe vou x, y, z befriedigt werden können, Gleichungen derselben Art ergeben, denen schon kleinere Werte von x, y, z genügen. Da man das angedeutete Verfahren fortsetzen kann, gelangt man nach einer endlichen Anzahl von Operationen zn einer Schlussgleichung mit solch kleinen Zahlengrössen x, y, z, für die die Unmögfichkeit des Bestehens unserer Gleichung

$x^n \pm y^n = z^n$ für $n = 4, 3, 14$ von selbst einleuchtet, woraus die Unmöglichkeit, die Gleichung $x^n \pm y^n = z^n$ für $n = 4, 3, 14$ durch grössere Zahlenwerte x, y, z zu erfüllen, folgt Umgekehrt sucht der französische Mathematiker Legendre zu zeigen, dass aus der Annahme, dass die Gleichung

$x^5 \pm y^5 = z^5$ durch ganze Zahlenwerte für x, y, z erfüllt werden kann, folgt, dass eine der Zahlengrössen x, y, z unendlich werden muss, woraus sich dann die Unmöglichkeit ergiebt, die Gleichung

$x^5 \pm y^5 = z^5$ durch endliche, ganze Zahlenwerthe für x, y, z zu befriedigen. Kommt aber in den bisher besprochenen Spezialbeweisen von Euler, Dirichlet und Legendre mehr oder weniger die Theorie der quadratischen Formen zur Anwendung, so sucht der französische Gelehrte Lamé auf ganz elementarem Wege zu zeigen, dass die Gleichung $x^7 + y^7 + z^7 = o$, wo z eine negative Grösse bedeuten soll, sich nicht durch ganze Zahl befriedigen lässt. Er beweist nämlich das Lemma, wonach der Quotient der Summe der drei Grössen x, y, z

$$x + y + z$$

und des Produktes aus den siebenten Wurzeln der Grössen

$$x + y, \ x + z, \ z + y$$

bezw. desselben Produktes multipliciert mit 7, je nachdem keine der drei Grössen $x, y, z \equiv o$ (mod. 7) oder eine derselben es ist, ein vollständiges Quadrat ist. Mit Hülfe des Lemmas gelingt es Lamé leicht den Nachweis zu führen, dass die Gleichung

$x^7 + y^7 + z^7 = o$ nicht durch ganze Zahlen befriedigt werden kann, wenn keine der drei Grössen $x, y, z \equiv o$ (mod. 7) ist. Ist aber eine der drei Grössen $x, y, z \equiv o$ (mod. 7), so führt Lamé vermittelst des bewiesenen Lemmas die Gleichung

$x^7 + y^7 + z^7 = o$ auf eine andere von der Form

$\zeta^4 = \xi^8 - 3\xi^4 \eta^4 + \frac{16}{7} \eta^8$ zurück, deren Unmöglichkeit

er nachweist. Der Vollständigkeit halber mögen die eben besprochenen Spezialbeweise von Euler, Dirichlet, Legendre und Lamé zum grössten Teil wenigstens ausgeführt werden:

α) Der Beweis Eulers für den Fall

$$n = 4.$$

Die zu betrachtende Gleichung ist in diesem Falle

$$x^4 + y^4 = z^4.$$

Da die Summe $x^4 + y^4$ ein Quadrat werden soll, folgt nach Euler, dass

$x^2 = p^2 - q^2$,
$y^2 = 2pq$; es ist dann wirklich
$x^4 + y^4 = (p^2 + q^2)^2$ ein Quadrat.

Aus den Gleichungen für x^2 und y^2 folgt, dass y grade, und weil x zu y relativ prim sein soll, dass x ungrade ist Da ferner $x^2 = p^2 - p^2$ ist, muss auch von den beiden Grössen p und q die eine grade, die andere ungrade sein. p kann nicht grade sein, weil dann $p^2 - q^2$ von der Form $4n + 3$ wird und deshalb nicht gleich dem Quadrat x^2 sein kann. Da nun $p^2 - q^2$ wiederum ein Quadrat werden soll, müssen sich zwei Grössen r, s finden lassen, so dass

$p = r^2 + s^2$, $q = 2rs$ wird, wo r und s wie p und q zu einander relativ prim sind. Wir erhalten dann:

$x^2 = (r^2 - s^2)^2$, $y^2 = 4rs\,(r^2 + s^2)$. Daraus ergiebt sich, weil r, s, $r^2 + s^2$ untereinander relativ prim sind, dass r, s, $r^2 + s^2$ Quadrate sein müssen. Setzt man

$r = t^2$, $s = u^2$, so muss auch $t^4 + u^4$ ein Quadrat sein. t und u sind aber kleiner als die entsprechenden Grössen x und y. Damit hat Euler den Beweis geliefert, dass es überhaupt keine Zahlen x und y giebt, die $x^4 + y^4$ zum Quadrat machen. Denn gäbe es zwei Biquadrate in grösseren Zahlen, deren Summe ein Quadrat wäre, so könnte man daraus eine Summe zweier weit kleinerer Biquadrate ableiten, die dieselbe Eigenschaft besässen, und so könnte man in dieser Schlussfolge fortfahren Da aber in kleinen Zahlen keine solche Summe möglich ist, kann sie es auch nicht in grossen sein. Aehnlich erledigt Euler den Fall, wenn es sich um die Gleichung

$x^4 - y^4 = z^4$ handelt.

β) Beweis Eulers, dass die Gleichung

$x^3 + y^3 = z^3$ durch ganze Zahlen nicht befriedigt werden kann.

Euler zeigt zuerst, dass man ohne Beschränkung der Allgemeinheit annehmen kann, dass in der Gleichung

1) $x^3 + y^3 = z^3$ die beiden Grössen x und y ungrade, z aber grade ist. Er führt dann für x und y folgende Werte

2) $x = p + q$, $y = p - q$, wo p und q ganze Zahlen bedeuten, von denen die eine grade, die andere ungrade ist. Die Werte von x und y setzen wir in unsere Gleichung (1) ein, und erhalten

3) $x^3 + y^3 = 2p^3 + 6pq^2 = 2p\,(p^2 + 3q^2) = z^3$.

Es müssen nun zwei Fälle unterschieden werden, je nachdem $z \equiv$ oder $\not\equiv o$ (mod. 3) ist.

Ist $z \not\equiv o$ (mod. 3), so sind die beiden Faktoren der rechten Seite unserer Gleichung (3) relativ prim zu einander, folglich ist 2p wie $p^2 + 3q^2$ ein Cubus.

Es muss deshalb folgende Gleichung bestehen

4) $p^2 + 3q^2 = [(t + u\sqrt{-3})\,(t - u\sqrt{-3})]^3$ oder

5) $\begin{cases} p + q\sqrt{-3} = (t + u\sqrt{-3})^3 \\ p - q\sqrt{-3} = (t - u\sqrt{-3})^3. \end{cases}$

Wir erhalten aus diesen Gleichungen durch Vergleichungen der reellen und imaginären Glieder auf beiden Seiten:

6) $p = t\,(t + 3u)\,(t - 3u)$ oder

$2p = 2t\,(t + 3u)\,(t - 3u)$. Wie sich leicht zeigen lässt, sind die drei Faktoren 2t, $t + 3u$ und $t - 3u$ relativ prim untereinander. Da aber 2p ein Cubus ist, muss jeder dieser Ausdrücke ein Cubus sein. Setzen wir also

7) $t + 3u = f^3$

8) $t - 3u = g^3$, so erhalten wir

9) $2t = f^3 + g^3$, wo 2t ein Cubus ist. Diese Gleichung (9) entspricht unserer Gleichuug (1)

$x^3 + y^3 = z^3$, nur dass die Zahlengrössen f, g $\sqrt[3]{2t}$ kleiner als die entsprechenden x, y, z sind.

Daraus schliesst Euler:

Wenn es zwei Cuben in grössern Zahlen giebt, deren Summe ein Cubus ist, so kann man daraus in kleinern Zahlen ebendergleichen anzeigen. Da es nun in kleinern Zahlen dergleichen nicht giebt, sind sie auch in grösseren Zahlen nicht vorhanden.

Ist zweitens $z \equiv o$ (mod. 3), so zeigt Euler auf eine ähnliche Weise die Unmöglichkeit der Gleichung

$$x^3 + y^3 = z^3.$$

Um Wiederholungen zu vermeiden, verweisen wir auf Eulers Algebra. (Leonhard Eulers vollständige Anleitung zur höhern und niedern Algebra, herausgegeben von Johann Gruson, Berlin 1796)

γ) Der Dirichletsche Beweis, dass die Gleichung

$x^{14} + y^{14} = z^{14}$ nicht durch ganze Zahlen befriedigt werden kann.

1) $x^{14} + y^{14} = z^{14}$ ist unsere zu untersuchende Gleichung. Da x, y, z untereinander relativ prim sind, müssen zwei der

Grössen ungrade, die dritte grade sein. Ist ferner eine der drei Grössen x, y, $z \equiv o$ (mod. 7), so kann es z nicht sein, weil die Summe von zwei Quadraten relativ primer Zahlen nicht durch 7 teilbar sein kann. Es kann demnach entweder x oder y nur durch 7 teilbar sein. wenn eine der Grössen x, y, $z \equiv o$ (mod. 7) ist.

α) Keine der drei Grössen x, y, z ist $\equiv o$ (mod. 7).

Aus der Gleichung (1) ergiebt sich auch folgende:

2) $y^{14} = z^{14} - x^{14} = (z^2 - x^2) [(z^2 - x^2)^6 + 7z^2 x^2 (z^4 - z^2 x^2 + x^4)]$.

Die Grössen zx, $z^2 - x^2$, $z^4 - z^2 x^2 + x^4$ sind relativ prim untereinander, weil es z und x sind.

Wir führen jetzt die Dirichletschen Abkürzungen ein:

3) $z^2 - x^2 = \varphi$

$zx (z^4 - z^2 x^2 + x^4) = \psi$. Die Gleichung (2) geht dann über in

4) $\varphi \, [(\varphi^3)^2 + 7\psi^2] = y^{14}$.

Die beiden Faktoren φ und $(\varphi^3)^2 + 7\psi^2$ sind zu einander relativ prim, deshalb ist jeder Faktor eine 14-te Potenz. Es muss daher folgende Gleichung sich ansetzen lassen:

5) $(\varphi^3 + \psi \sqrt{-7}) = (g + h \sqrt{-7})^{14}$. Durch Vergleichung der reellen und imaginaren Teile erhält man, dass $\psi \equiv o$ mod. 7 sein muss. Weil aber

$\psi = zx (z^2 - x^2)$ durch 7 nicht teilbar sein kann, ist für den Fall, dass keine der Zahlen

x, y, $z \equiv o$ (mod. 7) ist, die Unmöglichkeit der Gleichung $x^{14} + y^{14} = z^{14}$ erwiesen.

β) Ist aber eine der drei Grössen x, y, $z \equiv o$ (mod. 7), so kann es nur, wie oben gezeigt ist, y oder x sein.

Welche dieser Grössen wir $\equiv o$ mod. 7 annehmen, bleibt für den Beweis gleichgiltig. Es sei also

$y \equiv o$ mod. 7. Dann setzen wir

$y = 7w$ in unsere Gleichung (2) ein, wodurch wir erhalten:

2') $z^{14} - x^{14} = 7^{14} w^{14}$. Anstatt dieser Gleichung untersucht Dirichlet die allgemeinere

3) $z^{14} - x^{14} = 2^m \, 7^{1+n} \, w^{14}$, wo m und n ganze positive Zahlen incl. o bedeuten sollen.

Führen wir diese früheren Abkürzungen in unsere Gleichung (3) ein, so erhalten wir

4) $z^{14} - x^{14} = \varphi \, [(\varphi^3)^2 + 7\psi^2] = 2^m 7^{1+n} \, w^{14}$.

φ ist hier durch 7 teilbar; wir können deshalb $\varphi = 7\chi$ setzen und erhalten

5) $7^2\chi \, [\psi^2 + 7 \, (7^2\chi^3)^2] = 2^m \, 7^{1+n} \, w^{14}$.

$7^2\chi$ und $\psi^2 + 7 \, (7^2\chi^3)^2$ sind dann relativ prim. Daraus folgt, dass $\psi^2 + 7 \, (7^2\chi^3)^2$ eine 14 Potenz sein muss, während $7^2\chi$ das Produkt

einer 14-ten Potenz und dem Faktor $2^m 7^{1+n}$ ist.

Wir können also setzen:

6) $\psi + 7^2 \chi^3 \sqrt{-7} = (r + s\sqrt{-7})^{14}$. Aus dieser Gleichung ergiebt sich:

7) $7^2 \chi^3 = \frac{(r + s\sqrt{-7})^{14} - (r - s\sqrt{-7})^{14}}{2\sqrt{-7}}$. In dieser Glelchung ist r zu s relativ prim und $r \not\equiv o \pmod{7}$. Führt man noch folgende Abkürzungen ein:

$(r + 7s^2)(r^4 - 2 \cdot 7^2 r^2 s^2 + 7^2 s^4) = R$, so ergiebt sich aus (7):

8) $7^2 \chi^3 = 2 \cdot 7 . r . s [R^2 - (7 \cdot 4^3 r^3 s^3)^2]$ oder

9) $7^6 \chi^3 = 2 \cdot 7^5 r . s [R + 7 \cdot 4^3 r^3 s^3][R - 7 \cdot 4^3 r^3 s^3]$.

Die drei Faktoren der rechten Seite unserer Gleichung (9) $2 \cdot 7^5 r s$, $R + 7 (4rs)^3$ und $R - 7 (4rs)^3$ sind zu einander relativ prim, folglich erhalten wir, da $7^6 \chi^3$ von der Form

$2^{3m} 7^{3+3n} \times$ 42ten Potenz (aus $7^2 \chi$) ist, folgende Relationen aus (9):

10) $2 \cdot 7^5 r s = 2^{3m} 7^{3+3n} v'^{14}$

$R + 7 (4rs)^3 = t'^{14}$

$R - 7 (4rs)^3 = u'^{14}$ oder schliesslich

11) $t'^{14} - u'^{14} = 2^{9m+4} 7^{3n'+1} v'^{14}$. Diese Gleichung ist ganz so gebildet wie die Gleichung (4), nur dass die Grössen t', u', v' kleiner sind als die entsprechenden Grössen z, x, w. Daraus erschliesst Dirichlet auf dieselbe Weise, wie es Euler im Falle $n = 4$ und 3 gethan hat, die Unmöglichkeit der Gleichung (3) und daraus die der Gleichung (2').

δ) Der Legendresche Beweis für die Unmöglichkeit der Gleichung

1) $x^5 + y^5 + z^5 = o$.

Dass die obige Gleichung durch ganze Zahlen nicht befriedigt werden kann, wenn alle drei Grössen x, y, $z \not\equiv o \pmod{5}$ sind, deutet Legendre nur an, dagegen führt er einen strengen Beweis für die Unmöglickkeit unserer Gleichung (1), wenn eine der Grössen z. B. $x \equiv o \pmod{5}$ ist. Sein Beweis zerfällt in zwei Teile, je nachdem x grade oder ungrade ist. Da es uns nur darauf ankommt, das Beweisverfahren Legendres zu veranschaulichen, wollen wir uns begnügen, den ersten Teil des Legendreschen Beweises für ein grades x in abgekürzter Form darzustellen.

x sei also eine grade Zahl, die $\equiv o \pmod{5}$ ist. Wir setzen dann

2) $x = -5tr$, wo r eine positive, zu 5t relativ prime Zahl bedeuten soll, in die Gleichung (1) ein und erhalten:

3) $y^5 + z^5 = -x^5 = (5tr)^5$. Aus dieser Gleichung ergeben sich die Relationen

4) $\begin{cases} y + z = 5^4 t^5 \\ y^4 - y^3 z + y^2 z^2 - y z^3 + z^4 = 5 r^5. \end{cases}$ Da y und z ungrade sind, muss t grade sein. Die zweite Gleichung aus (5) lässt sich in folgende Form bringen:

$$6)\quad 5\left(\frac{y^2+z^2}{2}\right)^2 - \left(\frac{y^2+2yz+z^2}{2}\right)^2 = 5 r^5 \text{ oder}$$

da $y + z = 5^4 t^5$ ist,

$$7)\quad \left(\frac{y^2+z^2}{2}\right)^2 - 5\left(\frac{5^7 t^{10}}{2}\right)^2 = r^5.$$

Da die linke Seite unserer Gleichung die Form $p^2 - 5q^2$ hat und r ein Divisor von ihr ist, muss er dieselbe Form haben. Ist das der Fall, so werde ich zwei ganze Zahlen f und g finden können, so dass

8) $r = f^2 - 5g^2$. Setzt man ferner

9) $(f \pm g\sqrt{5})^5 = F \pm G\sqrt{5}$, so erhalte ich aus (8)

10) $r^5 = F^2 - 5G^2$. Aus der Gleichung (9) ergeben sich für F und G folgende Werte

11) $\begin{cases} F = f(f^4 + 50f^2 g^2 + 125g^4) \\ G = 5g(f^4 + 10f^2 g^2 + 5g^4). \end{cases}$ Um für G einen neuen Wert zu erhalten, setzt Legendre in die Gleichung (10) den Wert von r^5 aus (7) ein und sucht die allgemeine Lösung der daraus folgenden Gleichung:

$$12)\quad \left(\frac{y^2+z^2}{2}\right)^2 - 5\left(\frac{5^7 t^{10}}{2}\right)^2 = F^2 - 5G^2.$$

Zu diesem Zweck setzt Legendre

13) $\frac{y^2+z^2}{2} \pm \frac{5^7 t^{10}}{2}\sqrt{5} = (F + G\sqrt{5})\ (m + n\sqrt{5})$, wo m und n der Gleichung

$m^2 - 5n^2 = 1$ genügen sollen; das ist aber der Fall, wenn $(m \pm n\sqrt{5}) = (9 \pm 4\sqrt{5})^k$ ist, wo k eine ganze Zahl bedeutet. Des Weiteren führt nun Legendre aus, dass man sich auf die Werte von $k = o, 1, 2$ beschränken kann, und dass schliesslich nur die Werte $m = 1$, $n = o$ in Rechnung kommen, wenn man den Bedingungsgleichungen (11) für F und G genügen will. Aus der Gleichung (13) folgt durch Vergleichung der rationalen und irrationalen Glieder:

$$14)\quad \tfrac{1}{2}(y^2 + z^2) = m F + n G$$

$$\tfrac{1}{2}\, 5^7 t^{10} = m G + n F.$$

Da aber $m = 1$, $n = o$ werden muss, wird $G = \frac{1}{2} 5^7 t^{10}$. Mit dem Werte aus (11) für G erhalten wir folgende Gleichung

15) $g(f^4 + 10f^2 g^2 + 5g^4) = \frac{1}{2}\, 5^6 t^{10}$. Da g, wie sich zeigen

lässt, grade ist, die beiden Faktoren der linken Seite unserer Gleichung (15) aber relativ prim zu einander sind, erhält man, wenn man für $t = 2u\,r'$ einführt, aus (15) folgende Relationen:

$$16) \begin{cases} g = 5^6\,2^9\,u^{10} \\ f^4 + 10f^2 g^2 + 5g^4 = (f^2 + 5g^2)^2 - 5\,(2g)^2 = r'^{10}. \end{cases}$$

Die linke Seite unserer letzten Gleichung ist aber wiederum von der Form $p^2 - 5q^2$, folglich wird ihr Divisor r'^2 dieselbe Form besitzen. Indem nun Legendre

$$17) \begin{cases} r'^2 = f'^2 - 5g'^2 \text{ und} \\ r'^{10} = F'^2 - 5G'^2 \end{cases}$$

setzt, wo $f'\,g'\,F'\,G'$ den Grössen f, g, F und G entsprechen, zeigt er auf die eben angeführte Weise, dass man schliesslich wiederum zu einer der Gleichung (15) entsprechenden Gleichung in den Grössen $f'\,g'\,u$ kommt, aus der sich dieselben Folgen ziehen lassen. Das Verfahren kann bis ins Unendliche fortgesetzt werden, indem man $u = 2u'\,r''$, $u' = 2u''\,r'''$ u. s. f. hintereinander setzt. Legendre zeigt nun ausführlich, dass die Grössen r beständig wachsen, während die Grössen u sich schliesslich der Einheit als Grenze nähern können. Da aber $x = -5 \,.\, 2^k\, r\, r'\, r'' \ldots$ ist, folgert Legendre, dass x unendlich werden muss, unsere Gleichung (1) für endliche Grössen also nicht bestehen kann.

ε) Der Lamésche Beweis, dass die Gleichung

1) $x^7 + y^7 = z^7$ nicht durch ganze Zahlen befriedigt werden kann.

Der erste Teil des Laméschen Beweises beschäftigt sich mit dem Falle, wo ich die Gleichung (1)

$$x,\ y,\ z \not\equiv o \pmod{7} \text{ sind.}$$

$$2) \begin{cases} x7 = (z - y)\,[(z - y)^6 + 7\,(z - y)^5 y + 3 \,.\, 7\,(z - y)^4 y^2 \\ \quad + 5 \,.\, 7\,(z - y)^3 y^3 \\ \quad + 5 \,.\, 7 \,.\, (z - y)^2 y^4 + 3 \,.\, 7\,(z - y)\,y^5 + 7y^6] \\ \quad = (z - y)\,X \\ y7 = (z - x)\,[(z - x)^6 + 7x\,(z - x)^5 + 3 \,.\, 7\,(z - x)^4 x^2 \\ \quad + 5 \,.\, 7\,(z - x)^3 x^3 \\ \quad + 5 \,.\, 7\,(z - x)^2 x^4 + 3 \,.\, 7\,(z - x)\,x^5 + 7x^6] \\ \quad = (z - x)\,Y \\ z7 = (x + y)\,[(x + y)^6 - 7\,(x + y)^5 y + 3 \,.\, 7\,(x + y)^4 y^2 \\ \quad - 5 \,.\, 7\,(x + y)^3 y^3 + 5 \,.\, 7\,(x + y)^2 y^4 - 3 \,.\, 7\,(x + y)\,y^5 + 7\,y^6] \\ \quad = (x + y)\,Z. \end{cases}$$

Da x, y, z relativ prim untereinander sein sollen und $\not\equiv o$ mod. 7 sind, folgt, dass X, $x - y$, Z, $x + y$ und Y und $z - x$ relativ prim untereinander sind.

Führen wir jetzt nach Lamé folgende Grössen ein:

$$3)\ \left\{\begin{array}{l} x = m\mu \\ y = n\nu \\ z = p\rho \\ X = m^7 \\ Y = n^7 \\ Z = p^7 \\ z - y = \mu^7 \\ z - x = \nu^7 \\ x + y = \rho^7 \end{array}\right\}$$ wo μ, ν, ρ, m, n, p, p relativ prim untereinander sind.

Aus diesen Bestimmungsgleichungen (3) ergiebt sich folgende:

$$4)\ x + y - z = \mu\,(m - \mu^6) = \nu\,(n - \nu^6) = \rho\,(\rho^6 - p).$$

Die letzten drei Produktengleichungen in (4) müssen den gemeinschaftlichen Faktor $\mu\nu\rho$ enthalten, deshalb lässt sich aus den Gleichungen (4) folgende ableiten:

5) $\mu\,(m - \mu^6) = \nu\,(n - \nu^6) = \rho\,(\rho^6 - p) = A\mu\nu\rho$, wo A eine ganze Zahl bedeutet.

Da ferner

$$6)\ m = \mu^6 + A\nu\rho,\ n = \nu^6 + A\rho\mu,\ p = \rho^6 - A\mu\nu$$

und

$A\mu\nu\rho = x + y - z = \mu m + \nu n - \rho p + \mu^7 + \nu^7 + 3A\mu\nu\rho$ ist, erhalte ich schliesslich

(7) $\rho^7 - \mu^7 - \nu^7 = 2\ A\mu\nu\rho$. Es muss jetz nachgewiesen werden, dass A ein vollständiges Quadrat ist.

Es ist

$$8)\ \left\{\begin{array}{l} 2x = \mu^7 - \nu^7 + \rho^7 \\ 2y = -\mu^7 + \nu^7 + \rho^7 \\ 2z = \mu^7 + \nu^7 + \rho^7. \end{array}\right.$$

Diese Werte für x, y, z in unsere Gleichung (1) eingesetzt ergeben:

$$9)\ (\mu^7 - \nu^7 + \rho^7)^7 + (-\mu^7 + \nu^7 + \rho^7)^7 = (\mu^7 + \nu^7 + \rho^7)^7.$$

Führt man jetzt nach Lamé folgende Grössen ein:

10) $\mu^7 = a$, $\nu^7 = b$, $\rho^7 = c$, so erhalten wir unter Benutzung folgender identischen Gleichung

$$11)\ (c + b + a)^7 - (c - b + a)^7 + (c + b - a)^7$$
$$= 7 \,.\, 8abc\,[3\,(a^4 + b^4 + c^4) + 10(a^2b^2 + c^2a^2 + b^2c^2)]$$

aus den Gleichungen (10) und (11) folgende.

$$12)\ (c - b - a)^7 = 7\ .\ 8\ abc\ [3\ (a^4 + b^4 + c^{11})$$
$$+\ 10\ (a^2b^2 + c^3a^2 + b^2c^2)].$$

Da $(c - b - a) = 2A\mu\nu\rho$ ist, geht (12) über in:

$$13)\ 2^4\ A^7 = 7\,[3\,(a^4 + b^4 + c^4) + 10\,(a^2\,b^2 + b^2\,c^2 + c^2\,a^2)]$$

Aus dieser Gleichung folgt erstens, dass

$A \equiv o$ mod. 7 ist und zweitens, dass A ein vollständiges Quadrat ist. Lösen wir nämlich Gleichung (13) nach a^2 auf, so erhalten wir:

14) $3a^2 = -5(b^2 + c^2) + 2\sqrt{4b^4 + 5b^2c^2 + 4c^4 + \frac{3}{7}2^2A^7}$.

Da der Radikand notwendiger Weise ein Quadrat sein muss, können wir setzen:

$\sqrt{4b^4 + 5b^2c^2 + 4c^4 + \frac{3}{7}2^2A^7} = \varphi$, und, indem wir noch die Abkürzung $b^2 + c^2 = \psi$ einführen, erhalten wir aus (14)

15) $3a^2 = 2\varphi - 5\psi$. Es ist weiter

16) $\frac{12A^7}{7} = \varphi^2 + 3b^2c^2 - 4\psi^2$. Setze ich jetzt $\mu\nu\rho = P$, so erhalte ich aus den Gleichungen (7 u. 8) nach Einführung der Grössen a, b, c

17) $c - b - AP = a + AP = x$; aus dieser Gleichung ergiebt sich

18) $a = c - b - 2AP$

$a^2 = \psi - 2cb - 4AP(c - PA - b) = \psi - 2cb - 4APx$.

Dieser Wert für a^2 in (15) eingesetzt, ergiebt

19) $\varphi = 4\psi - 3cb - 6APx$. Setze ich diesen Wert von φ in (16) ein, so erhalte ich schliesslich:

20) $A\left[\frac{1}{7}A^6 + Px(4\psi - 3cb - 6APx)\right] = (\psi - cb)^2$

$= (b^2 - cb + c^2)^2$. Da die Faktoren der linken Seite unserer Gleichung relativ prim unter einander sind, folgt aus der Gleichung (20), dass A ein vollständiges Quadrat sein muss. Demnach muss sich $b^2 - cb + c^2$ in zwei Faktoren zerlegen lassen,

21) $b^2 - cb + c^2 = BG$ derart, dass $A = B^2$ und

$\frac{1}{7}A^6 + Px(4\psi - 3cb - 6APx)^2 = G^2$ ist.

Der Hauptteil des Laméschen Beweises ist jetzt erbracht. Setzen wir jetzt noch:

$D = G - 2PBA$, so erhalten wir aus den Gleichungen (2 und 7) durch Subtraktion:

22) $a^2 + b^2 + c^2 - bc - ca + ab = BD$. Nehmen wir noch die Gleichungen (7, 13) hinzu:

$abc = P^7$

$c - a - b = 2B^2P$ (Gl. 7).

$3(a^4 + b^4 + c^4)) + 10(a^2b^2 + c^2a^2 + b^2c^2) = \frac{16}{7}B^{14}$ (Gl. 13)

und eliminieren aus den 4 Gleichungen die Grössen a, b, c, so erhalten wir die Schlussgleichung:

23) $7\left(\frac{B^6}{7}\right) + P^8 = D^2 - 5B^3PD + 7B^6P^4$ oder

$P^2(7B^6P^2 - 5B^3D - P^6) = 7\left(\frac{B^6}{7}\right) - D^2$.

Lamé zeigt nun, dass die linke Seite der letzten Gleichung die Form 4n hat, während die rechte von der Form 4n + 2 ist Wir stossen also auf einen Widerspruch, woraus sich die Unmöglichkeit unserer Gleichung (1) ergiebt.

Der zweite Teil des Unmöglichkeitsbeweises der Gleichung $x^7 + y^7 = z^7$, wenn eine der Grössen x, y, $z = o$ (mod. 7) ist, basiert, wie wir schon erwähnt haben, darauf, dass Lamé zeigt, dass 7A ein vollständiges Quadrat ist, und mit Hülfe dieses Nachweises führt Lamé die Gleichung $x^7 + y^7 = z^7$ auf eine andere von der Form

$\zeta^4 = \xi^8 - 3\xi^4 \eta^4 + \frac{16}{7} \eta^8$ zurück, die durch ganze Zahl nicht befriedigt werden kann.

Lebesque und Genocchi suchen den Laméschen Beweis zu vereinfachen, indem sie die Gleichung $x^7 + y^7 = z^7$ auf Gleichungen niedrigen Grades zurückführen, die sich nicht durch ganze Zahlen befriedigen lassen. (S. des Näheren Journal de mathémat. Band 5, C. R. 82). —

ι) Der Kummersche Beweis des Fermatschen Satzes. Herrn Professor Kummer ist es gelungen, für eine Reihe von wohlcharakterisierten Primzahlen λ, die Unmöglichkeit der Gleichung $x^\lambda \pm y^\lambda = z^\lambda$ nachzuweisen, wenn x, y, z ganze Zahlen bedeuten, die nicht einmal reell zu sein brauchen. Sein Beweis gründet sich auf zwei Voraussetzungen über die Primzahl λ, zu deren Ergründung eine genauere Kenntniss der complexen Einheiten und der Formenanzahlen für die aus den λ-ten Wurzeln der Einheit gebildeten complexen Zahlen gehört. Die zwei Voraussetzungen sind, wie Herr Professor Kummer in den Berichten der königl. Akademie zu Berlin (1847) auseinandersetzt, folgende:

A) Es soll λ eine solche Primzahl sein, dass die Anzahl der nicht aequivalenten Formen, welche zu derselben gehören, nicht durch λ selbst teilbar sei, oder nach der Kummerschen Anschauungsweise: Es soll die Anzahl aller nicht aequivalenten idealen complexen Zahlen nicht durch λ teilbar sein, oder noch anders ausgesprochen: Es soll die λ-te Potenz einer idealen complexen Zahl niemals zu einer wirklichen werden.

B) Es soll λ eine solche Primzahl sein, dass jede complexe Einheit, welche für den Modul λ einer realen ganzen Zahl congruent wird, nur eine λ-te Potenz einer anderen Einheit sei, oder wenn $\alpha^\lambda = 1$ und $E(\alpha)$ und $e(\alpha)$ complexe Einheiten bezeichnen, dass die Congruenz $E(\alpha) \equiv c$ (mod. λ), wo c eine ganze reale Zahl bezeichnet, notwendig die Gleichung $E(\alpha) = (e(\alpha))^\lambda$ nach sich zieht.

Unter diesen Voraussetzungen beweist Professor Kummer zuerst, dass die Gleichung

$x^\lambda - y^\lambda = z^\lambda$ nicht in ganzen Zahlen bestehen kann, wenn keine der drei Grössen x, y, $z \equiv o$ mod. λ ist. Nach Erledigung dieses Falles beweist er, dass die Gleichung

$u^\lambda - v^\lambda = E(\alpha)(1-\alpha)^{n\lambda} w^\lambda$, in welcher unsere Gleichung $x^\lambda - y^\lambda = z^\lambda$ für $z \equiv o$ (mod. λ) enthalten ist, nicht für ganze Zahlen

bestehen kann, wenn dle Primzahl λ den beiden vorigen Voraussetzungen genügt. Wie aber Herr Professor Kummer in demselben Bande der Akademieberichte weiter ausführt, genügen alle Primzahlen λ, welche in den Zählern der ersten $\frac{\lambda - 3}{2}$ Bernouillischen Zahlen als Faktoren nicht vorkommen, diesen Voraussetzungen. Der Fermatsche Satz, insoweit er von Herrn Professor Kummer streng bewiesen ist, heisst also: Die Gleichung

$x^\lambda - y^\lambda = z^\lambda$, in welcher λ eine ungrade Primzahl ist, die in keiner der ersten $\frac{\lambda - 3}{2}$ Bernouillischen Zahlen als Faktor des Zählers vorkommt, ist in ganzen Zahlen unlösbar.

Zu den Zahlen λ, für welche der Kummersche Beweis gilt, gehören:

$\lambda = 3, 5, 11, 13, 17, 19, 23, 29, 31, 41, 43 \ldots$ Die Zahl 37 ist die kleinste von allen Primzahlen, für welche der Kummersche Beweis keine Geltung hat Herr Professor Kummer hat aber weiter durch Erforschungen der besonderen Eigenschaften, welche die complexen Zahlen besitzen, wenn die Klassenanzahl durch λ teilbar ist, die Richtigkeit des Fermatschen Satzes auch für diese Werte der Potenzexponenten λ zu ergründen gesucht. Da aber, wie Herr Professor Kummer in den Berichten der Akademie zu Berlin vom Jahre 1857 mitteilt, diese Untersuchung in ihrer ganzen Allgemeinheit grosse Schwierigkeiten darbietet, so beschränkte er sich darauf, den Fermatschen Satz für eine neue Reihe von Werten der λ, welche durch drei neue Voraussetzungen:

1) Der erste der beiden Faktoren, aus welchen die Klassenanzahl besteht, soll den Faktor λ einmal und nur einmal enthalten.
2) Es soll irgend einen Modul geben, für welchen die Einheit $E_\nu(\alpha)$ einer λ-ten Potenz nicht congruent ist,
3) Die $\nu\lambda$-te Bernouillische Zahl soll nicht congruent Null sein für den Modul λ^3;

vollständig charakterisiert sind, zu beweisen.

Dieser Reihe von Primzahlen λ gehören unter andern die drei Zahlen 37, 59, 67 an, die einzigen Primzahlen innerhalb des ersten Hundert, für welche der erste Kummersche Beweis nicht galt. Durch diesen letzteren Beweis ist der Fermatsche Satz für alle Primzahlen des ersten Hunderts bewiesen und wie Herr Professor Kummer zeigt, nicht bloss für reelle, sondern auch complexe Zahlen x, y, z.

VIII.

Nach Herrn Professor Kummer haben viele Mathematiker, wie die Herren Lefébure, Mansion, Mantone, Jonquières, Borletti, Catalan u. A. vergeblich versucht, den Fermatschen Satz auf elementarem Wege allgemein zu beweisen. Wir werden im Folgenden zwei vor nicht allzulanger Zeit veröffentlichte Beweise durchsprechen.

Der eine rührt von Herrn Lucas her und ist im 58ten Bande des Grunertschen Archivs zu finden. Herr Lucas will allgemein beweisen, dass die Gleichung 1) $x^n + y^n = z^n$ durch ganze Zahlen nicht gelöst werden kann. Je nachdem nun x die kleinste oder grösste Zahl von den drei Zahlenwerten x, y, z ist, setzt er

$z = x + a$, $y = x + b$ oder

$z = x - a$, $y = x - b$. Nehmen wir an, x sei die grösste Zahl, so erhalten wir aus der Gleichung (1)

2) $x^n = (x - a)^n + (x - b)^n$ oder

3) $x^n - \binom{n}{1}(a + b)x^{n-1} + \binom{n}{2}(a^2 + b^2)x^{n-2} - (1)^n(a^n + b^n) = o.$

Herr Lucas untersucht nun, ob diese Gleichung durch reelle Werte von x befriedigt werden kann. Die Gleichung haben die Wurzeln w_1, w_2 — w^n.

Dann ist bekanntlich

$$\sum_{k=1}^{n} w_k = \binom{n}{1}(a + b), \quad \sum_{(i \gtrless k = 1,2-n)} w_i\, w_k = \binom{n}{2}(a^2 + b^2) \text{ u. f. f.}$$

Wir erhalten daraus:

4) $\frac{1}{n}\sum_{k=1}^{n} w_k = (a + b)$, d. h. $\frac{1}{n}\sum_{k=1}^{n} w_k$ ist eine ganze Zahl, da a und b ganze Zahlen sind.

Aus der Gleichung folgt folgende:

$$5) \sum_{k=1}^{n} w_k^2 + 2 \sum_{(i \gtrless k = 1,2-n)} w_i\, w_k = n^2 (a + b)^2$$

Da aber $\sum_{(i \gtrless k = 1,2-n)} w_i\, w_k = \binom{n}{2}(a^2 + b^2)$ ist, so ergiebt sich

$$\frac{1}{n}\sum_{k=1}^{n} w_k^2 = n(a^2 + 2ab + b^2) - (n - 1)(a^2 + b^2)$$

$= a^2 + b^2 + 2n\,ab$ gleich einer ganzen Zahl. Herr Lucas behauptet nun, dass $\frac{1}{n}\sum_{k=1}^{n} w_k^2$ nur für $n = 1$ und 2 eine ganze Zahl sein könne, in allen andern Fällen nicht. Ein Beweis für seine Behauptung ist von ihm aber nicht gegeben, weshalb auch der Fermatsche Satz nicht für bewiesen erachtet werden kann.

Vor Kurzem wurde von Herrn Staatsrath Rieke im 34. Bande der Zeitschrift für Mathematik und Physik ein allgemeiner Beweis des Fermatschen Satzes veröffentlicht.

Herr Rieke geht von der bekannten Identitäts aus:

$$x^p + y^p = (x + y)^p + \sum_{q=1}^{\frac{p-1}{2}} (-1)^q \frac{p}{q} (p-q-1)_{q-1} (x+y)^{p-2q} x^q y^q$$

$$x^p - y^p = (x - y)^p + \sum_{q=1}^{\frac{p-1}{2}} \frac{p}{q} (p-q-1)_{q-1} (x-y)^{p-2q} x^q y^q,$$

um zu untersuchen, in welchem Falle die beiden Grössen $\frac{x^p \pm y^p}{x \pm y}$ und $x \pm y$ einen gemeinsamen Teiler haben können, wenn x und y relativ prim untereinander sind, und kommt dabei zu bekannten Resultaten. Sein Beweis zerfällt dann in zwei Teile, je nachdem keine der drei Grössen x, y, z $\equiv$ o (mod. p) oder eine es ist.

I. Keiner der drei Grössen x, y, z sei $\equiv$ o (mod. p). Es sind also x, y, z $\not\equiv$ o (mod. p), wo p eine ungrade Primzahl bedeutet.

Von den drei Grössen x, y, z, die relativ prim untereinander sein sollen, müssen zwei ungrade, die dritte grade sei. z sei nun grade

$$z = 2z_1.$$

Dann folgt aus der Gleichung

1) $x^p + y^p = z^p = (2z_1)^p$

2) $x + y = 2^p a^p$, wenn a ein Faktor von z_1 bedeutet.

$= 2A$, wenn

3) $A = 2^{p-1} a^p$.

Setzen wir 4) $x - y = 2B$, so wird B ungrade und relativ prim zu A sein. Die Gleichung (1) lässt sich aber dann in folgende Form bringen:

4) $z^p = 2^p z_1^p = (A + B)^p + (A - B)^p$

$= 2(A^p + (p)_2 A^{p-2} B^2 + (p)_4 A^{p-4} B^4 + \ldots (p)_{p-1} A B^{p-1})$

Dividieren wir die Gleichung (4) durch $2A - 2^p B^p$, so erhalten wir

5) $\left(\frac{z_1}{a}\right)^p = A^{p-1} + (p)_2 A^{p-3} B^2 + \ldots + (p)_{p-1} B^{p-1}$, wo

$\left(\frac{z_1}{a}\right)$ eine ganze Zahl ist.

$= A^{p-1} + p B^2 \varphi(A, B)$, wo $\varphi(A, B)$ eine ganze ganzzahlige rationale Funktion der Grössen A, B bedeutet. Wäre nun $B^2 \varphi(A, B) \equiv$ o (mod. p), so ergäbe sich aus der Gleichung (5) die Congruenz

6) $\left(\frac{z_1}{a}\right)^p - A^{p-1} \equiv$ o (mod. p^2). Diese Congruenz lässt sich aber leicht umformen in die Congruenz:

7) $\left(\frac{A}{a}\right)^p - A^{p-1} \equiv$ o (mod. p^2) oder

8) $A^{p-1}(2^{p-1}-1) \equiv o$ (mod. p^2). Da aber $A^{p-1} \not\equiv o$ (mod. p.) ist, erhält man schliesslich

9) $2^{p-1}-1 \equiv o$ mod. p^2, eine Congruenz, die unmöglich ist. Um also die Unmöglichkeit unserer Gleichung (1) nachzuweisen, müsste Herr Rieke zeigen, dass $B^2 \varphi(A, B) \equiv o$ (mod. p) ist. Zu diesem Zwecke zerlegt er die rechte Seite der Gleichung (5) in zwei Faktoren und erhält

$$7) \left(\frac{z_1}{a}\right)p = \left(A^{\frac{p-1}{2}} + B\sqrt{p}\,.\,\sqrt{\varphi(A,B\,i)}\right) \times$$
$$\left(A^{\frac{p-1}{2}} - B\sqrt{p}\ \sqrt{\varphi(A,B\,i)}\right)$$
$$= (\sqrt{e} + \sqrt{f}\,i)^p (\sqrt{e} - \sqrt{f}\,i)^p$$

Aus dieser Gleichung leitet Herr Rieke durch Vergleichung der reellen und imaginären Teile folgende ab:

$$8) B\sqrt{p}\,.\,\sqrt{\varphi(A,B)} = \sqrt{f}\,[(p)_1\, e^{\frac{p-1}{2}} - (p)_3\, e^{\frac{p-3}{2}} f_2$$
$$+ \ldots\ldots + (-1)^{\frac{p-1}{2}} f^{\frac{p-1}{2}}]$$

oder

$$9) B\sqrt{\varphi(A,B} = \sqrt{\frac{f}{p}}\,[(p)_1\, e^{\frac{p-1}{2}} \ldots + (-1)^{\frac{p-1}{2}} f^{\frac{p-1}{2}}]$$

Diese Gleichung veranlasst nun Herrn Rieke zu folgendem irrtümlichen Schluss: Da für diese Gleichung keine höhere Wurzel als die Quadratwurzel vorkommen darf, muss f den Faktor p enthalten und dann $B\varphi(A, B) \equiv o$ (mod. p) sein. Wieso aber unsere Gleichung (8), die durch Division mit $\sqrt{p}$ in (9) übergeht, eine höhere Wurzel als die Quadratwurzel enthält, zeigt Herr Rieke nicht; seine Schlussfolgerung kann demnach nicht für richtig angesehen werden und damit ist auch der erste Teil seines Beweises verfehlt.

II. Ebensowenig kann der zweite Teil seines Beweises für gelungen anerkannt werden, weil in diesen von Herrn Rieke irrationale Grössen bezüglich ihrer Teilbarkeit wie rationale behandelt werden.

Herr Rieke nimmt in dem zweiten Teile seines Beweises an, dass $x \equiv o$ mod. p ist. Dann zeigt er, dass

$$x + y = a^p,\ z - x = b^p,\ z - y = p^{p-1} c^p \text{ gesetzt}$$

werden können.

Unsere Gleichung (1) wird dann von ihm umgeformt in folgende:

$$2) \left(\frac{x}{pc}\right)^p = \frac{z^p - y^p}{p(z-y} = \frac{1}{p}\,[(z-y)^{p-1}$$
$$+ \sum_{q=1}^{\frac{p-1}{2}}{}' \frac{p}{q}(p-q-1)_{q-1}(z-y)^{p-2q-1} z^q y^q]$$
$$= \frac{V}{p}$$

V zerlegt Herr Rieke in die quadratischen Faktoren

$(z - y)^2 + m_1 zy, (z - y)^2 + m_2 zy, \ldots.$

wo die irrationalen Grössen $m_1, m_2 - m_{\frac{p-1}{2}}$ Wurzeln der Gleichung

$$m^{\frac{p-1}{2}} - \frac{p}{1}(p-2)_0 m^{\frac{p-3}{2}} ---- + (-1)^{\frac{p-1}{2}} p = o$$

sind. Herr Rieke begründet nun seinen Beweis, dass er aus dieser Gleichung die Folgerung zieht, dass die irrationale Grösse m den Faktor $p^{\frac{2}{p-1}}$ enthalten muss und daraus seine Schlüsse zieht, auf die wir nicht einzugehen brauchen, weil es nicht zulässig ist, von Faktoren irrationaler Grössen zu sprechen in dem Sinne, wie man es bei rationalen Grössen thut.

IX.

Zum Schlusse wollen wir noch einmal die Resultate zusammenstellen, die wir in unserer Arbeit gewonnen haben. Im Abschnitt V haben wir gezeigt, dass die Gleichung $x^{2n} \pm y^{2n} = z^{2n}$ nicht durch ganze Zahlen befriedigt werden kann, wenn n eine Primzahl von der Form $4k + 3$ ist. In den übrigen Abschnitten haben wir uns damit beschäftigt, zu zeigen, dass der Fermatsche Satz über die Gleichung $x^n + y^n = z^n$ ganz allgemein gilt, wenn z eine Primzahl oder eine Primzahl multipliciert mit 2 ist, oder schliesslich, wenn eine der drei Grössen x, y, z zu den Zahlenklassen gehört, die in dem Abschnitt VI charakterisiert sind. Zu diesen Zahlenklassen gehören aber die Zahlen 1 — 202, wie eine leichte Ueberlegung zeigt, folglich können wir den Satz aussprechen: Sind x, y oder z dem Zahlenintervall 1 — 202 entnommen, so kann die Gleichung

$x^n \pm y^n = z^n$ nicht bestehen.

Ich, Julius Rothholz, wurde am 6. Dezember 1864 zu Schwersenz, einer kleinen Stadt der Provinz Posen, als jüngster Sohn des Kaufmanns Fabisch Rothholz und seiner Ehefrau Johanna Rothholz, geboren. Den ersten Unterricht genoss ich in der jüdischen Elementarschule, die zur Zeit von den Herren Lesser und Grünfeld geleitet wurde. Dieselbe verliess ich im Jahre 1876, um in das Königliche Mariengymnasium zu Posen eintreten zu können. Nachdem ich hier Michaelis 1883 das Reifezeugniss für die Universität erhalten hatte, widmete ich mich dem Studium der Mathematik und Physik an der Universität Berlin und besuchte die Vorlesungen der Herren Professoren: Tobler, Netto, Hettner, Paulsen, Dilthey, Zeller, Fuchs, Knoblauch, Kronecker, Glan und Aron. Den genannten Herren sage ich an dieser Stelle meinen Dank, insbesondere aber fühle ich mich gedrungen, Herrn Prof. Dr. Netto für die mannigfachen Anregungen, die er mir bei vorliegender Arbeit zu Theil werden liess, auf's herzlichste zu danken.

Berlin, im Juli 1892.

Der Verfasser.


U. C. BERKELEY LIBRARIES
C052269420



